(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－289327

(43)公開日　平成11年(1999)10月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ

審査請求　未請求　請求項の数11　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－89097

(22)出願日　平成10年(1998)４月１日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　西村　拓也
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

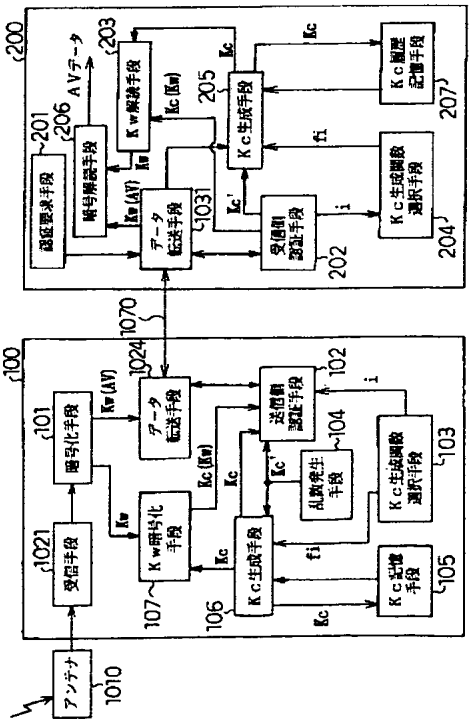
最終頁に続く

(54)【発明の名称】　データ送信装置、データ受信装置、及び媒体

(57)【要約】

【課題】コントロールキーＫｃが不正に解読されると、それで暗号化されているワークキーＫｗも解読されるため、ＡＶデータが不正に解読されるという課題。

【解決手段】ＳＴＢ１００は、受信手段１０２１からのＡＶデータをワークキーＫｗにより暗号化する暗号化手段１０１と、ＶＴＲ装置２００と認証動作を行い、Ｋｃの暗号化を行う送信側認証手段１０２と、Ｋｃを生成するために、複数個の関数とその関数識別子を予め内蔵し、何れかの関数を選択するＫｃ生成関数選択手段１０３と、Ｋｃを生成する際に利用する乱数Ｋｃ’を発生させる乱数発生手段１０４と、既に生成されたＫｃを記憶するＫｃ記憶手段１０５と、過去に生成されたＫｃの一部と、上記出力された乱数Ｋｃ’と、それらを変数とする上記選択された関数ｆｉとを利用して、新たなＫｃを生成するＫｃ生成手段１０６と、生成されたＫｃを用いてＫｗを暗号化するＫｗ暗号化手段１０７手段等を備える。



【特許請求の範囲】

【請求項１】　データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、
前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、
前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、
そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、
前記コントロールキーＫｃの生成に利用する秘密要素を発生させる秘密要素発生手段と、
過去に生成されたコントロールキーＫｃの全部又は一部と前記発生された秘密要素と、それらを変数とする第１の関数とを利用して、新たなコントロールキーＫｃを生成するコントロールキー生成手段とを備え、
前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第１の関数を有する前記データ受信装置に転送するものであることを特徴とするデータ送信装置。

【請求項２】　データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、
前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、
前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、
そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、
新たなコントロールキーＫｃを生成するコントロールキー生成手段と、
過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、
前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第２の関数の逆関数を有する前記データ受信装置に転送するものであることを特徴とするデータ送信装置。

【請求項３】　請求項１又は２記載のデータ送信装置にデータ転送要求を行う転送要求手段と、
前記転送要求に基づいて前記データ送信装置から転送されてくる暗号化されたワークキーＫｗを、コントロールキーＫｃで解読するとともに、暗号化されたデータを、そのワークキーＫｗに基づいて解読する暗号解読手段と、
前記ワークキーＫｗの解読に既に利用された前記コントロールキーＫｃを履歴情報として記憶する履歴情報記憶手段と、
前記第１の関数又は前記逆関数を格納する関数格納手段と、
前記格納されている第１の関数又は逆関数と、前記履歴情報記憶手段に記憶されている過去のコントロールキーＫｃの全部又は一部と、請求項１又は２記載の前記データ送信装置から転送されてくる前記秘密要素とに基づいて、新たなコントロールキーＫｃを生成するコントロールキー生成手段と、を備えたことを特徴とするデータ受信装置。

【請求項４】　前記データ送信装置が別のデータ受信装置と既に前記データの転送を行っている途中から、データの転送を要求する場合、
前記コントロールキー生成手段により初期段階で利用される前記過去のコントロールキーＫｃは、前記履歴情報記憶手段に記憶されている前記コントロールキーＫｃではなく、前記データ送信装置から転送されてくるコントロールキーＫｃであることを特徴とする請求項３記載のデータ受信装置。

【請求項５】　前記転送を行う旨が決定された場合、
前記データ受信装置が有する前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期においては、前記コントロールキーＫｃを含む暗号情報を初期情報として、前記データ受信装置に転送することを特徴とする請求項１又は２記載のデータ送信装置。

【請求項６】　前記転送を行う旨が決定された場合、
前記データ受信装置が有する前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期においては、前記秘密要素を含む前記不足している変数を初期情報として前記データ受信装置に転送することを特徴とする請求項１又は２記載のデータ送信装置。

【請求項７】　前記転送を行う旨が決定された場合、
前記データ受信装置が有する前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期の内、（１）前半においては、前記コントロールキーＫｃを含む暗号情報を初期前半情報として、又、（２）後半においては、前記秘密要素を含む前記不足している変数を初期後半情報として前記データ受信装置に転送することを特徴とする請求項１又は２記載のデータ送信装置。

【請求項８】　前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期においては、請求項５記載のデータ送信装置から転送されてくる前記初期情報を解読し、前記コントロールキーＫｃを抽出する抽出手段を備え、
前記暗号解読手段が、前記抽出されたコントロールキーＫｃを前記解読に利用することを特徴とする請求項３記載のデータ受信装置。

【請求項９】　前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している

時期においては、前記コントロールキー生成手段が、前記６記載のデータ送信装置から転送されてくる前記初期情報と、前記関数とを利用して、前記コントロールキーＫｃを生成することを特徴とする請求項３記載のデータ受信装置。

【請求項１０】　前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期の内、（１）前記前半においては、請求項６記載のデータ送信装置から転送されてくる前記初期前半情報が解読され、前記コントロールキーＫｃが抽出され、又、（２）前記後半においては、請求項６記載のデータ送信装置から転送されてくる前記初期後半情報と前記関数とを利用して、前記コントロールキーＫｃが生成されることを特徴とする請求項３記載のデータ受信装置。

【請求項１１】　請求項１～１０の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録したことを特徴とする媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ送信装置、データ受信装置、及び媒体に関する。

【０００２】

【従来の技術】従来より、衛星放送で送られてくるテレビ番組等を、衛星放送受信機（以下、これを単に、ＳＴＢと呼ぶ）により受信して、その受信機に接続されたＶＴＲ装置で録画したり、テレビで視聴したりすることが行われている。

【０００３】この場合、放送されてくる映像・音声データの中には、記録が禁止されているものや、１回だけ記録可能とされている条件付きデータがある。従って、これらの条件が守られる為には、この条件を正しく認識して、正規に動作する装置をユーザ側が使用することが前提となる。

【０００４】そこで、ＳＴＢから、例えばＶＴＲ装置に対して、１回のみ記録可能なデータを送信する場合、先ず、そのＶＴＲ装置が、上記の様な正規なＶＴＲ装置であるかどうかを確認するための認証・鍵交換（ＡＫＥ）動作が行われるのが通常である。

【０００５】そして、この認証作業が成立しなかった場合には、認証対象となったＶＴＲ装置を不正装置であると認定し、その様な不正装置に対しては、データの送信を行わないようにする。

【０００６】以下、図６を参照しながら、従来のＳＴＢと各端末装置との構成と、その認証動作を中心に説明する。

【０００７】図６は、従来のＳＴＢと、ＶＴＲ装置等の各端末装置との接続状況及び構成を示すブロック図である。

【０００８】同図に示す様に、アンテナ１０１０は、衛星からの放送電波を受信する手段であり、ＳＴＢ１０２０は、受信した放送電波をＡＶデータに変換する手段である。データ伝送ライン１０７０は、ＳＴＢ１０２０と、以下に述べる各端末装置とを間に設けられたデータ伝送のためのバスラインである。又、端末装置として、ＶＴＲ装置（Ａ）１０３０、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｃ）１０５０、更にＴＶ装置（Ｄ）が、データ伝送ライン１０７０によりＳＴＢ１０２０と接続されている。

【０００９】次に、同図を参照しながら、ＳＴＢ１０２０の内部構成について更に述べる。

【００１０】即ち、受信手段１０２１は、アンテナ１０１０と直結し、受信したデータの復調を行い、その受信データに施されている放送用スクランブルを解除し、更に、多重化されている受信データを分離する手段である。暗号化手段１０２２は、予め備えた暗号化のためのワークキーＫｗにより、受信手段１０２１から出力されてきたＡＶデータを圧縮状態のまま暗号化する手段である。又、コントロールキーＫｃは、ＳＴＢ１０２０に予め内蔵されており、ワークキーＫｗを暗号化手段により暗号化するための鍵である。更に又、暗号化手段１０２２は、認証手段１０２３により、後述する認証動作の結果生成されたサブキーを用いてコントロールキーＫｃを暗号化する手段である。

【００１１】認証手段１０２３は、ＡＶデータの転送要求をしてきた端末装置との間で、双方の装置が正規の装置であるかどうかを互いに確かめ合うため、所定の秘密関数を利用して認証作業を行い、その結果として、認証相手に対応したサブキーＫｓａを生成する手段である。又、認証手段１０２３は、あらゆる端末装置が有する固有の全ての秘密関数（Ｓａ，Ｓｂ，Ｓｃ，Ｓｄ，・・，Ｓｎ，・・・）を、それらの識別番号と対応させて保有している。データ転送手段１０２４は、ディジタル・インタフェースとして知られているＩＥＥＥ１３９４である。データ転送手段１０２４は、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない認証用データやコマンド等の転送に適したアシンクロナス転送の２つの転送を行う手段である。尚、上記暗号化されたＡＶデータは、暗号化手段１０２２からデータ転送手段１０２４へ送られる。又、上記暗号化されたワークキーや、暗号化されたコントロールキーは、認証手段１０２３からデータ転送手段１０２４へ送られる。

【００１２】尚、暗号化されたＡＶデータＫｗ（ＡＶ）、暗号化されたワークキーＫｃ（Ｋｗ）、そして暗号化されたコントロールキーＫｓａ（Ｋｃ）は、データ転送手段１０２４からＶＴＲ装置１０３０等の端末装置に送られる。

【００１３】次に、ＶＴＲ装置（Ａ）１０３０の内部構成について、更に述べる。

【００１４】同図に示すとおり、データ転送手段１０３

１は、データ転送手段１０２４と同様の手段であり、暗号化されたワークキー及び暗号化されたＡＶデータを受け取る手段である。認証手段１０３２は、固有の秘密関数Ｓａを予め有しており、認証作業の結果として、サブキーＫｓａを生成して、復号化手段１０３３へ出力する手段である。復号化手段１０３３は、データ転送手段１０３１から得た暗号化されたコントロールキーＫｓａ（Ｋｃ）をサブキーＫｓａにより復号し、この復号化されたコントロールキーＫｃにより、暗号化されたワークキーＫｃ（Ｋｗ）を復号し、その復号化されたワークキーＫｗにより、暗号化されたＡＶデータＫｗ（ＡＶ）を復号する手段である。記録・再生手段１０３４は、復号化されたＡＶデータを記録し、又、その記録データを再生する手段である。

【００１５】尚、その他の端末装置である、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｄ）１０５０、ＴＶ装置（Ｄ）１０６０も、記録・再生手段を除き、上記ＶＴＲ装置（Ａ）１０３０の構成と基本的に同じである。但し、各認証手段が予め有する秘密関数は、上記各装置の順番でいえば、Ｓｂ、Ｓｃ、Ｓｄである。従って、各装置と、ＳＴＢ１０２０との認証作業により生成されるサブキーは、上記の順番でいえば、Ｋｓｂ、Ｋｓｃ、Ｋｓｄである。

【００１６】以上の構成において、次に、認証・鍵交換の内容を簡単に述べる。尚、本明細書では、認証の成立の結果としてサブキーＫｓｘを生成するまでの作業、及びその後に行うコントロールキーＫｃの転送・受理の作業を含む一連の作業をまとめて、認証・鍵交換というものとする。

【００１７】例えば、ＶＴＲ装置（Ａ）１０３０からＳＴＢ１０２０に対して、ＡＶデータの転送要求を行う場合、その実行に先立ち次のような複雑な認証作業が必要となる。

【００１８】ステップ１００１：即ち、先ず、ＶＴＲ装置（Ａ）１０３０の認証手段１０３２が、乱数Ａ１，Ａ２を発生させ、これを秘密関数Ｓａにより暗号化する。ここで、暗号化された乱数をＳａ（Ａ１，Ａ２）と記載する。認証手段１０３２は、Ｓａ（Ａ１，Ａ２）と自己の識別番号ＩＤａとをデータ転送手段１０３１を介して、ＳＴＢ１０２０へ転送する。ここで、識別番号は、各端末装置固有の番号で予め与えられている。

【００１９】ステップ１００２：ＳＴＢ１０２０では、認証手段１０２３がデータ転送手段１０２４を介して、Ｓａ（Ａ１，Ａ２）と識別番号ＩＤａとを得て、その識別番号を認識して、それに対応する秘密関数Ｓａを、保有している複数の秘密関数の中から選択する。これにより、ＳＴＢ１０２０が、ＶＴＲ装置（Ａ）１０３０との間で認証に使用すべき秘密関数が特定される。

【００２０】ステップ１００３：次に、ＳＴＢ１０２０の認証手段１０２３が、秘密関数Ｓａを用いて、上記受信したＳａ（Ａ１，Ａ２）を解読し、Ａ１，Ａ２を復元して、後者の乱数Ａ２のみを、暗号化せずにＶＴＲ装置（Ａ）１０３０へ送り返す。

ステップ１００４：次に、ＶＴＲ装置（Ａ）１０３０の認証手段１０３２が、ＳＴＢ１０２０から送り返されてきた乱数Ａ２と、自らが、上記ステップ１００１で発生させた乱数Ａ２とを比較する。双方の乱数が一致すれば、ＳＴＢ１０２０が正規の装置であると判断出来る。

【００２１】ステップ１００５：次に、ＳＴＢ１０２０側の認証手段１０２３が、乱数Ｂ１，Ｂ２を発生させ、これを秘密関数Ｓａにより暗号化する。そして、Ｓａ（Ｂ１，Ｂ２）をＶＴＲ装置（Ａ）１０３０へ転送する。

【００２２】ステップ１００６：ＶＴＲ装置（Ａ）１０３０では、認証手段１０３２が秘密関数Ｓａを用いて、上記受信したＳａ（Ｂ１，Ｂ２）を解読し、Ｂ１，Ｂ２を復元して、後者の乱数Ｂ２のみを、暗号化せずにＳＴＢ１０２０へ送り返す。

【００２３】ステップ１００７：次に、認証手段１０２３が、ＶＴＲ装置（Ａ）１０３０から送り返されてきた乱数Ｂ２と、自らが、上記ステップ１００５で発生させた乱数Ｂ２とを比較する。双方の乱数が一致すれば、ＶＴＲ装置（Ａ）１０３０が正規装置であると判断出来る。

【００２４】以上により、認証が成立したことになり、双方が互いに相手装置が正規の装置であることを確認出来る。その結果、ＶＴＲ装置（Ａ）１０３０へのＡＶデータの転送が許可される。

【００２５】この認証作業の結果、４つの乱数Ａ１，Ａ２とＢ１，Ｂ２が、双方の装置の認証手段１０２３，１０３２に発生している。

【００２６】そこで、次に、双方の認証手段１０２３，１０３２がそれぞれ、乱数Ａ１，Ｂ１を用いて上記サブキーＫｓａを生成する。尚、サブキーＫｓａの生成に際し、乱数Ａ２，Ｂ２を使用しないのは、これらは、暗号化せずに転送されたという経緯があるため、その様な経緯の無い乱数Ａ１，Ｂ１を使用する方が、キーの安全性から見て、より優れているからである。

【００２７】暗号化手段１０２２では、この様にして生成されたサブキーＫｓａを用いて、コントロールキーＫｃが暗号化され、又、コントロールキーＫｃを用いてワークキーＫｗが暗号化される。これらは、認証手段１０２３へ送られる。又、ＡＶデータはワークキーＫｗで暗号化されて、データ転送手段１０２４へ送られる。

【００２８】そして、上記暗号化されたコントロールキーＫｓａ（Ｋｃ）と、暗号化されたワークキーＫｃ（Ｋｗ）が、認証手段１０２３からデータ転送手段１０２４を介してＶＴＲ装置（Ａ）１０３０へ転送される。その後、暗号化されたＡＶデータＫｗ（ＡＶ）がデータ転送手段１０２４から、ＶＴＲ装置（Ａ）１０３０へ転送さ

れる。

【００２９】一方、ＶＴＲ装置（Ａ）１０３０では、復号化手段１０３３が、先ず、認証手段１０３２から得たサブキーＫｓａを用いて、暗号化されたコントロールキーＫｓａ（Ｋｃ）の復号を行う。次に、復号されたコントロールキーＫｃを用いて暗号化されたワークキーＫｃ（Ｋｗ）の復号を行う。更に、この様にして復号されたワークキーＫｗを用いて、暗号化されたＡＶデータＫｗ（ＡＶ）を復号するものである。

【００３０】尚、ＳＴＢ１０２０が、使用するワークキーＫｗは、転送データの安全性を確保するために、データ転送中において定期的に変更される。

【００３１】従って、ワークキーＫｗが変更される度に、暗号化された新たなワークキーＫｗが、ＳＴＢ１０２０からデータ転送中の端末装置へ送られる。

【００３２】

【発明が解決しようとする課題】しかしながら、このような従来のデータ転送のやり方では、仮に、コントロールキーＫｃが不正者によって解読されたとすると、コントロールキーＫｃで暗号化されているワークキーＫｗも解読されてしまうため、結果的に、暗号化されたＡＶデータが、不正者によって解読されることになるという課題を有していた。

【００３３】この場合、コントロールキーＫｃを更新することが考えられるが、上述したとおり、従来は、認証・鍵交換の一環として、コントロールキーＫｃを転送するものであるから、ただ単にコントロールキーＫｃを更新するとなると、認証・鍵交換の動作を更新の度に行う必要がある。

【００３４】しかし、認証・鍵交換の動作をＫｃの更新の度に再度行うとなると、新たなサブキーを生成するまでの上記一連の処理等が、双方の装置にとって大きな負担となる。そこで、本願発明者は、認証・鍵交換の動作による負担を従来に比べて実質上増やすことなく、コントロールキーＫｃを更新することにより、コントロールキーＫｃのセキュリティーを向上することを考えたものである。

【００３５】本発明は、上述した課題を考慮して、従来に比べて実施上の負担を増やすことなくコントロールキーＫｃの秘密保持についての信頼性を従来に比べてより一層向上させることが出来るデータ送信装置、データ受信装置、及び媒体を提供することを目的とする。

【００３６】

【課題を解決するための手段】請求項１記載の本発明は、データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、前記コントロールキーＫｃの生成に利用する秘密要素を発生させる秘密要素発生手段と、過去に生成されたコントロールキーＫｃの全部又は一部と前記発生された秘密要素と、それらを変数とする第１の関数とを利用して、新たなコントロールキーＫｃを生成するコントロールキー生成手段とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第１の関数を有する前記データ受信装置に転送するものであるデータ送信装置である。

【００３７】請求項２記載の本発明は、データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、新たなコントロールキーＫｃを生成するコントロールキー生成手段と、過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第２の関数の逆関数を有する前記データ受信装置に転送するものであるデータ送信装置である。

【００３８】請求項３記載の本発明は、請求項１又は２記載のデータ送信装置にデータ転送要求を行う転送要求手段と、前記転送要求に基づいて前記データ送信装置から転送されてくる暗号化されたワークキーＫｗを、コントロールキーＫｃで解読するとともに、暗号化されたデータを、そのワークキーＫｗに基づいて解読する暗号解読手段と、前記ワークキーＫｗの解読に既に利用された前記コントロールキーＫｃを履歴情報として記憶する履歴情報記憶手段と、前記第１の関数又は前記逆関数を格納する関数格納手段と、前記格納されている第１の関数又は逆関数と、前記履歴情報記憶手段に記憶されている過去のコントロールキーＫｃの全部又は一部と、請求項１又は２記載の前記データ送信装置から転送されてくる前記秘密要素とに基づいて、新たなコントロールキーＫｃを生成するコントロールキー生成手段とを備えたデータ受信装置である。

【００３９】請求項１１記載の本発明は、上記の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録した媒体である。

【００４０】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００４１】（第１の実施の形態）図１は、本発明の一

実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の構成について述べる。尚、本実施の形態では、図６で説明したものと、基本的に同じ構成のものには、同じ符号を付し、その詳細な説明は省略した。

【００４２】図１に示すＳＴＢ１００には、既に述べた図６と同様に、データ受信端末装置としてＶＴＲ装置（ａ）２００、ＶＴＲ装置（ｂ）３００、記録装置（ｃ）４００及びＴＶ装置（ｄ）５００が接続されている構成である。尚、図１では、説明の都合上、端末装置としてＶＴＲ装置（ａ）２００のみを記載し、他の端末装置の記載を省略した。これら記載を省略した端末装置３００～５００は、以下に述べるＶＴＲ装置（ａ）２００の構成と基本的に同様の構成を備えている。

【００４３】同図において、先ず、ＳＴＢ１００の構成を述べる。

【００４４】即ち、暗号化手段１０１は、受信手段１０２１からのＡＶデータをワークキーＫｗにより暗号化する手段である。送信側認証手段１０２は、端末装置との間で認証・鍵交換を行う手段である。又、送信側認証手段１０２は、認証動作においてサブキーを生成し、初回のみ、その生成したサブキーを用いて複数個のコントロールキーＫｃを暗号化する手段である。Ｋｃ生成関数選択手段１０３は、コントロールキーＫｃを生成するために、f_1～f_mのm個の関数と、それに対応する関数識別子１～ｍを予め内蔵しており、何れか一つの関数f_iを選択する手段である。又、Ｋｃ生成関数選択手段１０３は、Ｋｃ生成手段１０６に対しては、選択した関数f_iを出力し、送信側認証手段１０２に対しては、対応する関数識別子ｉを出力する手段である。乱数発生手段１０４は、コントロールキーＫｃの生成に利用される乱数Ｋｃ’を発生し、出力する手段である。Ｋｃ記憶手段１０５は、既に生成されたコントロールキーＫｃを記憶する手段である。Ｋｃ生成手段１０６は、Ｋｃ記憶手段１０６から送られてくる、過去に生成された幾つかのコントロールキーＫｃの一部と、上記出力された乱数Ｋｃ’と、それらを変数とする上記出力された関数f_iとを利用して、新たなコントロールキーＫｃを生成する手段である。ここで、関数ｆｉの変数となるコントロールキーＫｃの一部とは、本実施の形態では、１つ前と、２つ前に生成したキーである。尚、この関数については、更に後述する。Ｋｗ暗号化手段１０７は、生成されたコントロールキーＫｃを用いてワークキーＫｗを暗号化する手段である。

【００４５】本実施の形態では、コントロールキーＫｃが、次々と更新されるので、データ転送の開始に際し、最初に使用されるコントロールキーをＫｃ〔１〕と表し、更新の結果、ｎ番目に使用されるコントロールキーをＫｃ〔ｎ〕と表すものとする。又、同様にして、Ｋｃ〔ｎ＋１〕を生成するために利用された乱数をＫｃ’〔ｎ〕と表すものとする。但し、ｎは、自然数とする。

【００４６】従って、本実施の形態では、上記関数ｆｉは、次のような式（数１）で表せる。

【００４７】

【数１】ｆｉ（Ｋｃ’〔ｎ〕，Ｋｃ〔ｎ－１〕，Ｋｃ〔ｎ〕）

ここで、ｎは、自然数とする。

【００４８】よって、ｎ＋１番目に生成されるコントロールキーＫｃ〔ｎ＋１〕は、次の式（数２）で表せる。

【００４９】

【数２】Ｋｃ〔ｎ＋１〕＝ｆｉ（Ｋｃ’〔ｎ〕，Ｋｃ〔ｎ－１〕，Ｋｃ〔ｎ〕）

ここで、ｎは、自然数とする。

【００５０】尚、本発明の転送要求受付手段は、データ転送手段１０２４及び送信側認証手段１０２を含む手段である。又、本発明のデータ転送手段は、データ転送手段１０２４及び暗号化手段１０１を含む手段である。本発明の第１暗号化手段は、暗号化手段１０１に、又、第２暗号化手段は、Ｋｗ暗号化手段１０７に対応する。本発明の秘密要素発生手段は、乱数発生手段１０４に対応し、本発明の第１関数は、関数f_iに対応する。また、送信側認証手段１０２は、図６で述べた認証手段１０２３と同様に、秘密関数（Ｓａ、Ｓｂ、Ｓｃ、Ｓｄ、・・・、Ｓｘ）を有している。

【００５１】次に、ＶＴＲ装置２００の構成について述べる。

【００５２】即ち、同図において、認証要求手段２０１は、ＳＴＢ１００に対して、データ転送の要求をするために認証要求を行う手段である。受信側認証手段２０２は、ＳＴＢ１００との間で認証・鍵交換を行う手段である。又、受信側認証手段２０２は、認証動作においてサブキーを生成し、認証動作の結果として送られてくる、暗号化された複数個のコントロールキーＫｃをそのサブキーにより解読し、その解読結果の中から、コントロールキーＫｃ〔１〕を抽出し、Ｋｗ解読手段２０３に出力する手段である。又、受信側認証手段２０２は、暗号化されたワークキーＫｗを受理して、Ｋｗ解読手段２０３に送る手段である。更に又、受信側認証手段２０２は、ＳＴＢ１００から送られてくる関数識別子ｉをＫｃ生成関数選択手段２０４に、又、乱数Ｋｃ’〔ｎ〕をＫｃ生成手段２０５に出力する手段である。

【００５３】暗号解読手段２０６は、ＳＴＢ１００から転送されてきた暗号化されたＡＶデータをワークキーＫｗを用いて解読し、記録・再生手段（図示省略）１０３４へ出力する手段である。Ｋｃ生成関数選択手段２０４は、ＳＴＢ１００が内蔵している上記複数個の関数と同じ関数を、予め内蔵しており、入力されてきた関数識別子ｉに対応する関数ｆｉを抽出して、Ｋｃ生成手段２０５へ出力する手段である。この関数ｆｉは、数１で表せる。Ｋｃ生成手段２０５は、Ｋｃ履歴記憶手段２０７か

ら読み出した１つ前と２つ前に使用していたコントロールキーＫｃと、受信側認証手段２０２から出力された乱数Ｋｃ’とを、関数ｆｉの変数として利用して、新たなコントロールキーＫｃを生成する手段である。この新たなＫｃは、数２で表せる。又、Ｋｃ履歴記憶手段２０７は、Ｋｃ生成手段２０５により生成されたコントロールキーＫｃの履歴を記憶しておく手段である。尚、ＳＴＢ１００と他の端末装置との間で、既にデータの転送が行われている最中に、ＶＴＲ装置２００が途中からデータの転送を受ける場合には、Ｋｃ履歴記憶手段２０７は、次のような例外的な動作を行う手段である。即ち、その場合、Ｋｃ履歴記憶手段２０７は、上記他の端末装置との間で現に使用しているコントロールキーと、その１つ前に使用していたコントロールキーとをＳＴＢ１００から受け取り、それらを記憶する手段である。

【００５４】尚、受信側認証手段２０２は、図６で述べた、認証手段１０３２と同様に、秘密関数Ｓａを有している。

【００５５】以上の構成において、次に、図１、図２を参照しながら、本実施の形態の動作を説明する。

【００５６】ここでは、まず、（１）ＳＴＢ１００が、ＶＴＲ装置２００のみに対してＡＶデータの転送を開始する場合を述べ、その後、（２）上記（１）の動作中に、別の受信端末装置すなわち、記録装置４００に対するデータ転送が開始される場合を中心に説明する。

【００５７】（１）上述した通り、ここでは、ＳＴＢ１００からＶＴＲ装置２００へのみ、ＡＶデータを転送する場合について述べる。

【００５８】ＶＴＲ装置２００が、所望のＡＶデータをＳＴＢ１００から転送してもらうためには、ＳＴＢ１００とＶＴＲ装置２００との間で、図６で述べたのと同様の認証・鍵交換の動作を行った後、本実施の形態の特有の動作を行うものである。

【００５９】ステップ１０１：即ち、ここでは、認証要求手段２０１により、ＳＴＢ１００に対して認証・鍵交換の動作の開始の要求が行われる。その後の認証・鍵交換の動作の詳細は、以下の点を除き、上述したステップ１００１～１００７で述べたものと同様であるので、その説明は省略する。尚、この認証・鍵交換の動作においては、ＶＴＲ装置２００における乱数Ａ１，Ａ２の発生は、受信側認証手段２０２が行い、ＳＴＢ１００における乱数Ｂ１，Ｂ２の発生は、乱数発生手段１０４が行う。又、上記ステップ１００１～１００７の動作において、認証が成立した場合、図６で述べた通り、双方の装置においてサブキーＫｓａが生成される。その後の、認証・鍵交換の動作において最初にＶＴＲ装置２００へ転送されるキーは、本実施の形態では、ステップ１０２で述べるように２個であり、この点は従来と異なる。

【００６０】ステップ１０２：即ち、乱数発生手段１０４で発生された２つの乱数をダミーキーＫｃ〔０〕と、コントロールキーＫｃ〔１〕と定義する。このダミーキーＫｃ〔０〕と、コントロールキーＫｃ〔１〕は、送信側認証手段１０２へ送られる。又、コントロールキーＫｃ〔１〕は、Ｋｗ暗号化手段１０７にも送られる。

【００６１】即ちこの場合、Ｋｃ〔０〕、及びＫｃ〔１〕の生成については、数２を使用せず、例外的処置として、乱数発生手段１０４により発生される乱数を使用するものとする。

【００６２】ステップ１０３：さらに、これら２つのキーＫｃ〔０〕及びＫｃ〔１〕は、Ｋｃ記憶手段１０５に記憶される。又、Ｋｃ生成関数選択手段１０３により選択された関数ｆｉが、Ｋｃ生成手段１０６に送られ、それに対応する関数識別子ｉが送信側認証手段１０２に送られる。尚、関数ｆｉは、必要に応じて、更新しても良い。

【００６３】ステップ１０４：送信側認証手段１０２では、上記のようにして送られてきたダミーキーＫｃ〔０〕とコントロールキーＫｃ〔１〕が、サブキーＫｓａにより暗号化されて、Ｋｓａ（Ｋｃ〔０〕，Ｋｃ〔１〕）として、データ転送手段１０２４へ送られる。さらに、Ｋｓａ（Ｋｃ〔０〕，Ｋｃ〔１〕）は、データ転送手段１０２４から、ＶＴＲ装置２００へ転送される。図２では、この転送に、符号６０１を付した。ここで、図２は、コントロールキーの更新に伴い行われる、ＳＴＢ１００から受信端末装置２００、４００への転送の状況を中心に示した模式図である。同図において、縦軸は時間であり、図中の上から下へ向けて時間が経過している。

【００６４】尚、この転送６０１の際、Ｋｃ生成関数ｆｉに対応する関数識別子ｉも、ＶＴＲ装置２００に転送される。

【００６５】ステップ１０５：ＳＴＢ１００から転送されてきたＫｓａ（Ｋｃ〔０〕，Ｋｃ〔１〕）と関数識別子ｉは、データ転送手段１０３１により、受信側認証手段２０２へ送られる。

【００６６】ステップ１０６：そして、受信側認証手段２０２は、Ｋｓａ（Ｋｃ〔０〕，Ｋｃ〔１〕）を解読し、前後に配置された２つのキーの内、予め定められている通り、後ろに配置されたＫｃ〔１〕を抽出し、Ｋｗ解読手段２０３へ送る。又、受信側認証手段２０２は、関数識別子ｉをＫｃ生成関数選択手段２０４へ送る。そして、Ｋｃ生成関数選択手段２０４が、その識別子ｉに対応する関数ｆｉを抽出して、Ｋｃ生成手段２０５へ送る。尚、解読されたＫｃ〔０〕，Ｋｃ〔１〕は、共に、Ｋｃ生成手段２０５を介して、Ｋｃ履歴記憶手段２０７に送られ、記憶される。

【００６７】ステップ１０７：一方、Ｋｗ暗号化手段１０７がコントロールキーＫｃ〔１〕を用いて暗号化したワークキー、即ち、Ｋｃ〔１〕（Ｋｗ）は、送信側認証手段１０２及びデータ転送手段１０２４を経て、ＶＴＲ装置２００に転送される。

【００６８】ステップ１０８：ＶＴＲ装置２００に送ら

れてきたＫｃ〔1〕（Ｋｗ）は、受信側認証手段２０２を経て、Ｋｗ解読手段２０３に送られる。Ｋｗ解読手段２０３は、ステップ１０６において送られてきたコントロールキーＫｃ〔1〕を用いて、Ｋｃ〔1〕（Ｋｗ）を解読して、Ｋｗを暗号解読手段２０６に送る。

【００６９】ステップ１０９：一方、ＳＴＢ１００の暗号化手段１０１により暗号化されたＡＶデータであるＫｗ（ＡＶ）の転送が、データ転送手段１０２４を介して開始される。

【００７０】ステップ１１０：Ｋｗ（ＡＶ）は、データ転送手段１０３１から暗号解読手段２０６へ送られる。暗号解読手段２０６は、Ｋｗ解読手段２０３から送られてきたＫｗを用いて、Ｋｗ（ＡＶ）を解読し、記録・再生手段に出力する。

【００７１】次に、ステップ１１０において、解読されたＡＶデータが記録・再生手段に出力されている途中で、コントロールキーＫｃが更新される場合の動作を述べる。

【００７２】ステップ２０１：本実施の形態では、コントロールキーを定期的に更新するものとし、乱数発生手段１０４が、乱数Ｋｃ’を定期的に発生させる。即ち、１回目の更新に利用する乱数Ｋｃ’〔1〕が、乱数発生手段１０４からＫｃ生成手段１０６と、送信側認証手段１０２に送られる。

【００７３】ステップ２０２：送信側認証手段１０２に送られた乱数Ｋｃ’〔1〕は、データ転送手段１０２４を介して、ＶＴＲ装置２００へ転送される。図２では、この転送に符号６０２を付した。

【００７４】ステップ２０３：Ｋｃ生成手段１０６は、Ｋｃ記憶手段１０５に記憶されているＫｃ〔0〕及びＫｃ〔1〕を読み出して、乱数発生手段１０４から送られてきた乱数Ｋｃ’〔1〕と共に、関数ｆｉ（数２参照）の変数として用いる。

【００７５】この場合、生成される新たなコントロールキーＫｃ〔2〕は、数２より、Ｋｃ〔2〕＝ｆｉ（Ｋｃ’〔1〕，Ｋｃ〔0〕，Ｋｃ〔1〕）と表せる。尚、Ｋｃ〔2〕は、Ｋｃ記憶手段１０５に記憶される。

【００７６】ステップ２０４：新たなコントロールキーＫｃ〔2〕は、Ｋｗ暗号化手段１０７へ送られ、ワークキーＫｗの暗号化に用いられる。暗号化されたワークキーであるＫｃ〔2〕（Ｋｗ）は、ステップ１０７と同様にしてＶＴＲ装置２００へ転送される。

【００７７】ステップ２０５：又、ステップ２０２において、ＶＴＲ装置２００に転送された乱数Ｋｃ’〔1〕は、データ転送手段１０３１から受信側認証手段２０２に送られ、さらにＫｃ生成手段２０５に送られる。

【００７８】ステップ２０６：Ｋｃ生成手段２０５では、Ｋｃ履歴記憶手段２０７に記憶されているＫｃ〔0〕及びＫｃ〔1〕と読み出して、ステップ２０５において送られてきた乱数Ｋｃ’〔1〕と共に、関数ｆｉ（数２参照）の変数として用いる。この場合、生成される新たなコントロールキーＫｃ〔2〕は、ステップ２０３で述べたものと同じであり、Ｋｃ〔2〕＝ｆｉ（Ｋｃ’〔1〕，Ｋｃ〔0〕，Ｋｃ〔1〕）と表せる。尚、Ｋｃ〔2〕は、Ｋｃ履歴記憶手段２０７に記憶される。

【００７９】ステップ２０７：新たなコントロールキーＫｃ〔2〕は、Ｋｗ解読手段２０３へ送られ、Ｋｃ〔2〕で暗号化されたワークキーＫｗの解読に用いられる。解読されたワークキーＫｗは暗号化解読手段２０６に送られる。

【００８０】ステップ２０８：ステップ１１０と同様の動作が行われる。

【００８１】次に、ステップ２０８において、解読されたＡＶデータが記録・再生手段に出力されている途中で、コントロールキーＫｃ〔2〕が、さらに更新される場合の動作を述べる。ここでは、すでに述べた内容と同様の点が多いので、数２に関する特徴点のみについて述べる。

【００８２】即ち、ここで生成されるコントロールキーＫｃ〔3〕は、数２のｎに２を代入することにより次のように表せる。図２では、乱数Ｋｃ’〔2〕の転送に符号６０３を付した。

【００８３】

【数３】

Ｋｃ〔3〕＝ｆｉ（Ｋｃ’〔2〕，Ｋｃ〔1〕，Ｋｃ〔2〕）

上記（数３）及び（数２）から明らかなように、本実施の形態においては、２回目の更新以降に生成されるコントロールキーは、１つ前、及び２つ前に使用したコントロールキーと、乱数発生手段１０４により更新の度に発生される乱数Ｋｃ’と、それらを変数とする関数ｆｉとにより生成されるものである。

【００８４】以上述べた様に、本実施の形態によれば、認証動作を繰り返すことなく、過去に使用したコントロールキーの履歴と乱数とを用いてコントロールキーを更新することにより、コントロールキーの信頼性をより一層向上させることが出来る。

【００８５】（２）上記（１）の動作において、コントロールキーの２回目の更新が行われた後に、記録装置４００に対するデータ転送が開始される場合について、図２を参照しながら述べる。

【００８６】ステップ３０１：ＳＴＢ１００と、新たに転送要求を行う記録装置４００との間において、ステップ１０１と同様の認証動作が行われる。

【００８７】ステップ３０２：認証が成立した後、送信側認証手段１０２は、Ｋｃ記憶手段１０５に記録されている、現在使用中のコントロールキーＫｃ〔3〕とその１つ前に使用していたコントロールキーＫｃ〔2〕とを読み出して、サブキーＫｓｃにより暗号化する。そして、このＫｓｃ（Ｋｃ〔2〕、Ｋｃ〔3〕）と、現在使用中の関数ｆｉに対応する関数識別子ｉとをデータ転送手段１０２

４を介して、記録装置４００へ転送する（図２では、この転送に符号６０４を付した）。尚、サブキーＫｓｃは、上記認証動作により上記と同様の方法により生成されたものである。

【００８８】ステップ３０３：記録装置４００では、受信側認証手段２０２が、上記のようにして送られてきたＫｓｃ（Ｋｃ〔2〕、Ｋｃ〔3〕）を、サブキーＫｓｃを用いて解読し、Ｋｃ〔3〕を抽出する。この解読・抽出の動作と、その後のＫｃ生成関数選択手段２０４及びＫｃ履歴記憶手段２０７などの動作は、ステップ１０６で述べた内容と同じである。

【００８９】ステップ３０４：一方、ＳＴＢ１００では、Ｋw暗号化手段１０７が、現在使用中のコントロールキーＫｃ〔3〕を用いて、ワークキーＫwを暗号化したＫｃ〔3〕（Ｋw）を記録装置４００に転送する。このＫｃ〔3〕（Ｋw）は、ＶＴＲ装置２００に転送したものと同じである。

【００９０】ステップ３０５：記録装置４００での、Ｋｃ〔3〕（Ｋw）の解読動作は、ステップ１０８の内容と同じである。

ステップ３０６：暗号化されたＡＶデータの転送動作は、ステップ１０９の内容と同じである。

【００９１】ステップ３０７：記録装置４００での、ＡＶデータの解読動作は、ステップ１１０の内容と同じである。

【００９２】次に、コントロールキーＫｃ〔3〕が更新される場合の動作は、上記ステップ２０１～２０８での説明において、Ｋｃ〔0〕をＫｃ〔2〕と読み替え、Ｋｃ〔1〕をＫｃ〔3〕と読み替え、かつ、乱数Ｋｃ’〔1〕を乱数Ｋｃ’〔3〕と読み替えたものと同じである。

【００９３】ここで生成されるコントロールキーＫｃ〔4〕は、数２のｎに３を代入することにより次のように表せる。図２では、乱数Ｋｃ’〔3〕の転送に符号６０５を付した。

【００９４】

【数４】

Ｋｃ〔4〕＝ｆｉ（Ｋｃ’〔3〕，Ｋｃ〔2〕，Ｋｃ〔3〕）

この様に、途中からＡＶデータの転送を受ける端末装置が現れて、受信端末が増加しても、ＳＴＢ１００が使用するコントロールキーは、受信端末装置の数に関係なく共通したものとなる。

【００９５】これにより、不正者が、たまたま、これまで使用されてきたコントロールキーの内、いずれか一つを、例えば、総当たり計算等により解いたとしても、それまでのコントロールキーの履歴と、それとは別の乱数との組み合わせにより、コントロールキーが生成されるため、不正解読されたコントロールキー以降に生成されたコントロールキーが連鎖的に解かれてしまうことを防止出来る。

【００９６】又、コントロールキーの更新に使用する乱数Ｋｃ’が、不正者により傍受されたとしても、それ以前のコントロールキーの履歴が分からなければ、コントロールキーの解読は不可能である。

【００９７】尚、上記実施の形態では、先に発生させた乱数と、過去のコントロールキーＫｃとを利用して、関数ｆｉ（第１の関数）により新たなコントロールキーＫｃを生成する場合について述べたが、これに限らず例えば、次の様な構成のデータ送信装置としても良い。即ち、具体的には、図３に示す様に、上記Ｋｃ生成手段１０６に代えて、（1）新たなコントロールキーＫｃを生成するコントロールキー生成手段１１０６と、上記乱数発生手段１０４に代えて、（2）過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数Ｆｉとを利用して、秘密要素Ｋｃ’を生成する秘密要素生成手段１１０４とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素Ｋｃ’を、前記第２の関数の逆関数F^{-1}ｉを有するデータ受信装置１２００に転送する構成のデータ送信装置１１００であっても良い。一方、データ受信装置１２００には、図３に示すように、第２関数選択手段１１０３が有する複数個の第２関数に対応する逆関数を備えた逆関数選択手段１２０４が設けられている。この逆関数選択手段１２０４は、受信側認証手段２０２からの関数識別子ｉを得て、それに対応する逆関数F^{-1}ｉを選択し、Ｋｃ生成手段２０５へ送る。Ｋｃ生成手段２０５は、送られてきた逆関数F^{-1}ｉを用いて、受信側認証手段２０２からの秘密要素Ｋｃ’と過去のコントロールキーＫｃを変数として、上記と同様に新たなコントロールキーＫｃを生成する。

【００９８】又、上記実施の形態では、認証が成立した場合、初回の転送６０１（図２参照）で、ワークキーＫwの暗号化に最初に使用するコントロールキーＫｃ〔1〕と、そのコントロールキーの更新に利用するキーＫｃ〔0〕とを暗号化して転送する場合について述べたが、これに限らず例えば、データ受信装置が有する第１の関数（例えば、関数ｆｉ）または上記逆関数F^{-1}ｉの変数がコントロールキーＫｃを生成するのに不足している時期においては、前記コントロールキーＫｃを含む暗号情報を初期情報として、前記データ受信装置に転送する構成のデータ送信装置であっても良い。即ち、具体的には、例えば、図４に示すように、ＳＴＢ２１００は、転送１６０２において、Ｋｓａ（Ｋｃ〔1〕，Ｋｃ〔2〕）を転送する。転送１６０２では、すでに行った認証・鍵交換により生成されたサブキーＫｓａをそのまま使用するので、新たなサブキーの生成作業は不要である。データ受信装置としてのＶＴＲ装置２２００は、転送されてきたＫｓａ（Ｋｃ〔1〕，Ｋｃ〔2〕）を解読し、Ｋｃ〔2〕を抽出する。

【００９９】又、これとは別の例として、データ受信装

置が有する第１の関数ｆｉ又は上記逆関数F^{-1}ｉの変数が、コントロールキーＫｃを生成するのに不足している時期においては、秘密要素（例えば、乱数Ｋｃ’）を含む前記不足している変数を初期情報として前記データ受信装置に転送する構成のデータ送信装置であってもよい。即ち、具体的には、図５に示すように、例えば、上記実施の形態の（数２）を利用した場合について述べると、次の式（数５）により表せるコントロールキーＫｃが、双方の装置において、関数ｆｉを利用して生成されるものである。

【０１００】

【数５】

Ｋｃ〔１〕＝ｆｉ（Ｋｃ’〔０〕，Ｋｃ〔－１〕，Ｋｃ〔０〕）

ここで、Ｋｃ’〔０〕は、データ送信装置で発生された乱数等の秘密要素であり、Ｋｃ〔－１〕、Ｋｃ〔０〕は、それまでに未使用のコントロールキーである。これら未使用のコントロールキーは、乱数として発生させても良いし、予め、内蔵されている複数個の中から抽出しても良い。この場合、図５に示す転送２６０１において、データ送信装置としてのＳＴＢ３１００からデータ受信装置としてのＶＴＲ装置３２００に対して、コントロールキーＫｃ〔１〕の生成に必要な変数として、Ｋｃ’〔０〕とＫｃ〔－１〕とＫｃ〔０〕とをサブキーにより暗号化して転送する必要がある。

【０１０１】又、これとは別の例として、データ受信装置が有する第１の関数又は上記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期の内、（１）前半においては、前記コントロールキーＫｃを含む暗号情報を初期前半情報として、又、（２）後半においては、前記秘密要素を含む前記不足している変数を初期後半情報として前記データ受信装置に転送する構成のデータ送信装置であってもよい。即ち、具体的には、図２の転送６０１に代えて、Ｋｓａ（Ｋｃ〔１〕）を転送し、同図の転送６０２に代えて、秘密要素としてのＫｃ’〔１〕と、上記不足している変数としてのＫｃ〔０〕とを転送するものである。これにより、転送６０１の結果、データ受信装置においてＫｃ〔１〕が抽出され、最初のコントロールキーとして使用される。又、データ受信装置では、この様にして抽出されたコントロールキーＫｃ〔１〕と、転送６０２により入手したＫｃ’〔１〕及びＫｃ〔０〕とを変数として、関数ｆｉにより次のコントロールキーＫｃ〔２〕を生成する。

【０１０２】又、上記実施の形態では、Ｋｃ生成関数を予め複数個有しており、その中から一つを選択して使用する場合について述べたが、これに限らず例えば、認証動作の際に、使用する関数そのものを転送する構成でも良いし、あるいは、関数は、はじめから固定されていても良い。

【０１０３】又、上記実施の形態では、先に発生させた乱数と、過去のコントロールキーＫｃとを利用して、関数ｆｉ（第１の関数）により新たなコントロールキーＫｃを生成する場合について述べたが、これに限らず例えば、新たなコントロールキーＫｃを生成するコントロールキー生成手段と、過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第２の関数の逆関数を有するデータ受信装置に転送する構成のデータ送信装置であっても良い。

【０１０４】又、上記実施の形態では、新たなコントロールキーＫｃを生成する際、コントロールキーＫｃの履歴として、１つ前と２つ前のものを変数として用いる場合について述べたが、これに限らず例えば、過去に使用したコントロールキーであれば、２つ前と３つ前、若しくは、１つ前と３つ前等どれでも良い。又、過去のコントロールキーＫｃであれば、その個数は、２個に限らず、例えば、１個以上であれば、幾つでも良く、記憶容量が確保出来るならば、過去に使用した全てのコントロールキーを用いてもかまわない。

【０１０５】又、以上述べた実施の形態の何れか一つに記載の各手段またはステップの全部又は一部の手段またはステップをコンピューターに実行させるためのプログラムを記録した磁気記録媒体や光記録媒体などを作成し、これを利用して上記と同様の動作を実行させることも出来る。この場合も上記と同様の効果を発揮する。

【０１０６】又、上記実施の形態の各手段又はステップの処理動作は、コンピュータを用いてプログラムの働きにより、ソフトウェア的に実現してもよいし、あるいは、上記処理動作をコンピュータを使用せずに特有の回路構成により、ハード的に実現してもよい。

【０１０７】

【発明の効果】以上述べたところから明らかなように本発明は、従来に比べて実質上の負担を増やすことなくコントロールキーの秘密保持についての信頼性を従来に比べてより一層向上させることが出来るという長所を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図

【図２】同実施の形態において、コントロールキーの更新に伴い行われる、ＳＴＢから受信端末装置への転送の状況を中心に示した模式図

【図３】本発明の他の実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図

【図４】本発明の別の実施の形態において、コントロールキーの更新に伴い行われる、ＳＴＢから受信端末装置への転送の状況を中心に示した模式図

【図５】本発明のさらに別の実施の形態において、コン

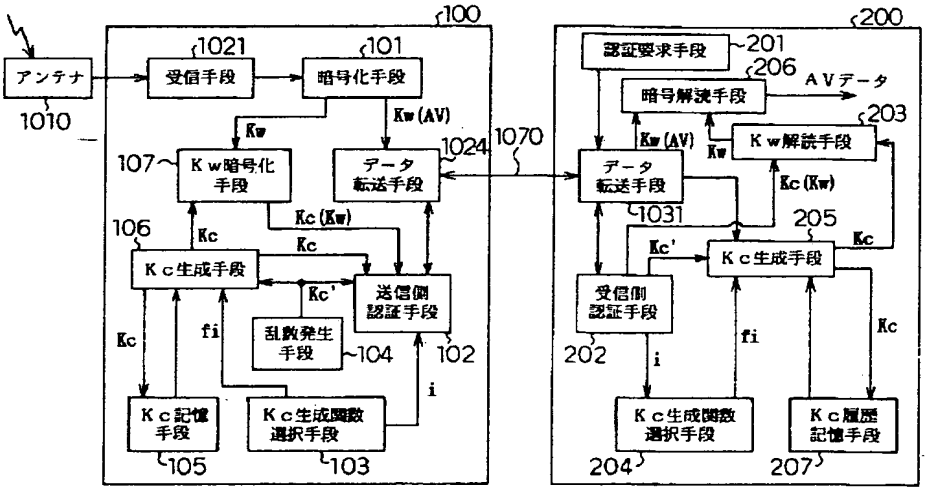
トロールキーの更新に伴い行われる、ＳＴＢから受信端末装置への転送の状況を中心に示した模式図

【図６】従来のデータ送信装置及びデータ受信装置の構成を示す構成図

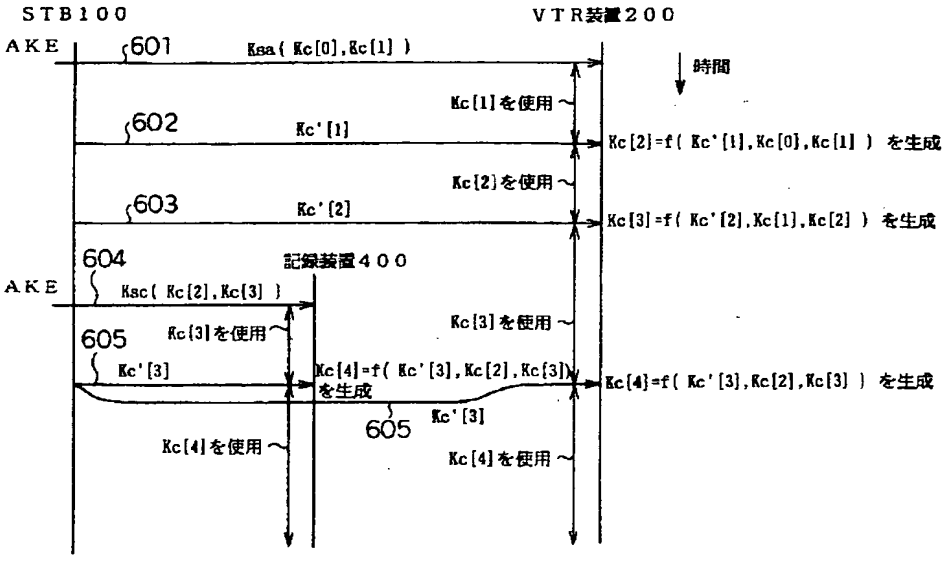
【符号の説明】

１００　ＳＴＢ
１０１　暗号化手段
１０２　送信側認証手段
１０３　Ｋｃ生成関数選択手段
１０４　乱数発生手段
１０５　Ｋｃ記憶手段
１０６　Ｋｃ生成手段
１０７　Ｋｗ暗号化手段

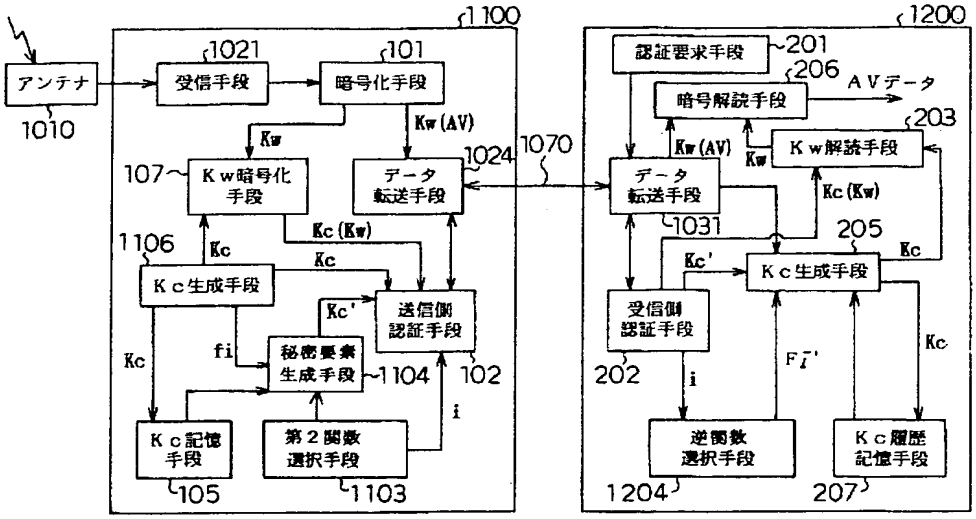
【図１】



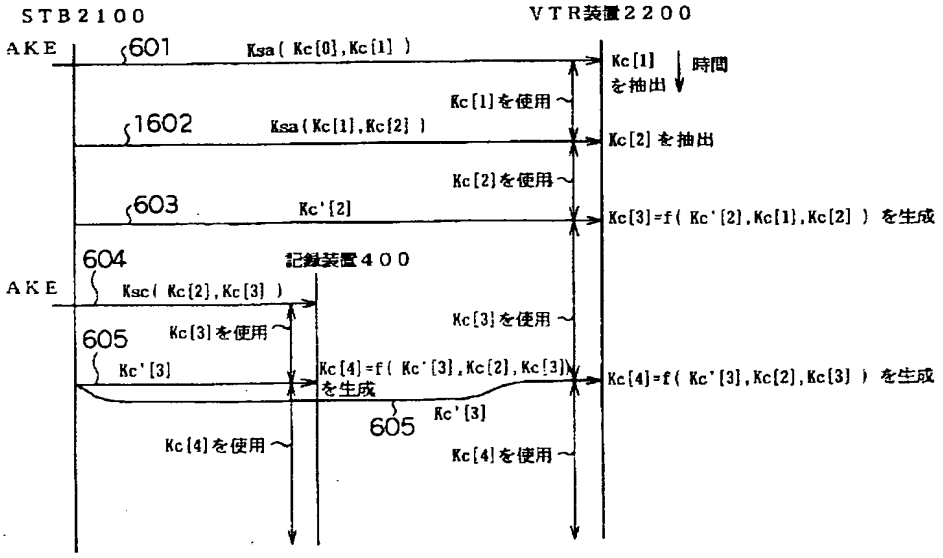
【図２】



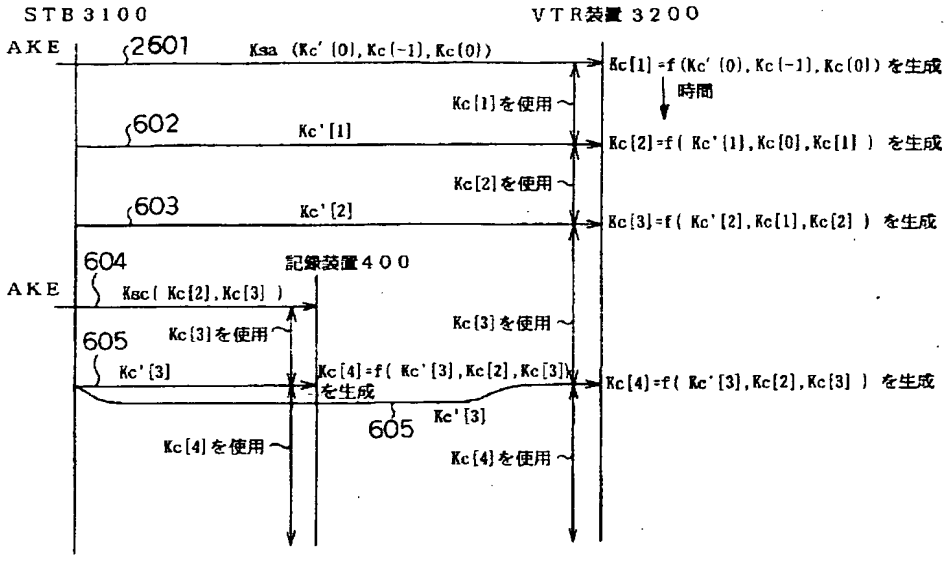
【図３】


1100
1200
アンテナ
1010
受信手段
1021
暗号化手段
101
Kw
Kw(AV)
Kw暗号化手段
107
データ転送手段
1024
1070
Kc(Kw)
Kc
1106
Kc生成手段
Kc'
送信側認証手段
fi
秘密要素生成手段
1104
102
i
Kc記憶手段
105
第２関数選択手段
1103
認証要求手段
201
206
AVデータ
暗号解読手段
203
Kw解読手段
データ転送手段
1031
205
Kc生成手段
受信側認証手段
202
逆関数選択手段
1204
Kc履歴記憶手段
207

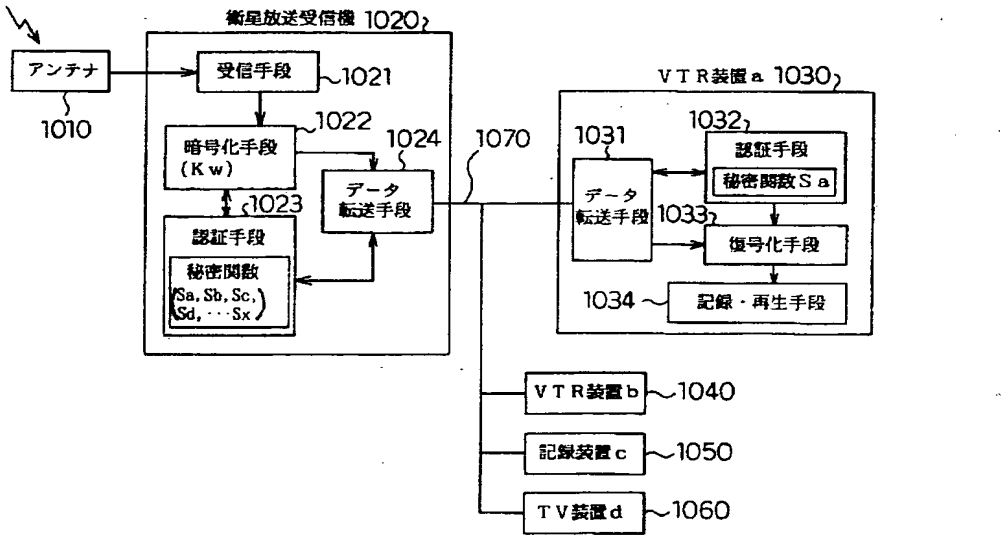
【図４】


STB2100
VTR装置2200
AKE
601
Ksa(Kc[0],Kc[1])
Kc[1]を抽出
時間
Kc[1]を使用
1602
Ksa(Kc[1],Kc[2])
Kc[2]を抽出
Kc[2]を使用
603
Kc'[2]
Kc[3]=f(Kc'[2],Kc[1],Kc[2]) を生成
604
記録装置400
AKE
Ksc(Kc[2],Kc[3])
Kc[3]を使用
Kc[3]を使用
605
Kc'[3]
Kc[4]=f(Kc'[3],Kc[2],Kc[3])を生成
Kc[4]=f(Kc'[3],Kc[2],Kc[3]) を生成
605
Kc'[3]
Kc[4]を使用
Kc[4]を使用

【図５】



【図６】



フロントページの続き

(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内